ANDREW MANCILLA
ROBERT M. FANTONE
Mancilla and Fantone, LLP
260 Madison Avenue, 22nd Floor
New York, New York 10016
Phone: 646-225-6686
Fax: 646-655-0269
Email: andrew@law-mf.com

Counsel for Defendant Karim Baratov

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. KARIM BARATOV, Defendant.	CASE NO. 3:17-CR-103 VC Sentencing Date: May 29, 2018 Time: 10:30 a.m. Court: Honorable Vince Chhabria

DEFENDANT'S SECOND MEMORANDUM OF LAW IN SUPPORT OF SENTENCING

PRELIMINARY STATEMENT

This case is about a young man, younger than most of the defendants in hacking cases throughout this country, who hacked emails, one at a time, for $100 a hack. He did not earn by stealing from anyone, but by being paid for a service. Albeit stupid and immature, he began when he was 12 years old and so continuing into his teens was less of a choice and more of a natural progression of his skills. Albeit reckless, whether he hacked 1,000 or 11,000, his mindset was the same, and thus the difference in imprisonment between 45 months and 94 months, offers no additional specific or general deterrence.

With respect to § 3553(a)(6), Mr. Baratov provides cases indicating that a sentence of 45 months is consistent with the sentences of similarly situated individuals. The Government's Supplemental Sentencing Memorandum (Dkt. 43) (herein cited as "Dkt. 43") fails to offer any insight as to the appropriate sentence for Mr. Baratov. First, the Sentencing Commission data the Government provides is unaccompanied by a description of the underlying conduct of the cases, thereby rendering the Government unable to meaningfully compare the data to Mr. Baratov's case. Second, the Government's analysis is based on the Sentencing Commission data fails to account for the Government's discretion in plea negotiations. Third, the 14 cases the Government cites are highly distinguishable from Mr. Baratov's.

Additionally, the Government does not attempt to address other factors under § 3553, including Mr. Baratov's young age and the jurisdictional issues uniquely present in this case due to more than 80% of Mr. Baratov's hacks have no nexus to the United States. For these reasons, Mr. Baratov respectfully asserts that a sentence of 45 months incarceration is sufficient, but not greater than necessary, to accomplish the sentencing goals described under the relevant statutory regime.

DISCUSSION

In Court on April 24, 2018, the Government repeatedly recognized – on the record – the guidelines' inability to appropriately measure culpability in cases, such as Mr. Baratov's, that involve instances of loss that may be difficult to calculate. However, despite the Government's failure to identify or calculate any actual harm caused by Mr. Baratov's conduct, the Government boisterously assures the Court that the instant guideline range "incorporates the § 3553(a) analysis with respect to the instant offense," (Dkt. 43 at 13; *see also* Dkt. 17).

With respect to the instant matter, the $500 presumed loss per access device mandated by 2B1.1 application note (F)(i) is the driving force behind Mr. Baratov's elevated sentencing guideline range. The concomitant more than $3 million loss amount accounts for 18 of the 27 total offense level, which underlies the Government's disproportional 94-month request. The USSG's $500 presumed loss provision is particularly troubling in the instant matter where the Government has not provided any evidence of loss actually suffered by any of the victims, and has accordingly requested no restitution.

As the 6th Circuit has noted, elevated sentences due to the $500 presumed loss provision could cause sentences calculated under the USSG to run afoul of § 3553(a)'s parsimony provision:

> The $500 rule first appeared in the Guidelines in 2000. The Commission added what is now § 2B1.1 cmt. n. 3(F)(i) after the Wireless Telephone Protection Act instructed it to "provide an appropriate penalty for offenses involving the cloning of wireless telephones." Pub. L. No. 105–172, § 2(e), 112 Stat. 53, 55 (1998). The Commission did not limit its change to wireless-telephone cloning, but amended the commentary to encompass all access devices. It explained that "the Commission's research and data supported increasing the minimum loss amount, previously provided only in § 2B1.1 (Larceny, Embezzlement, and Other Forms of Theft), from $100 to $500 per access device," U.S.S.G. Supp. App. C, Amend. 596, but the Commission did not elaborate upon the substance of its "research and data."
>
> Theoretically, the $500 fictional amount should have to pass muster under the parsimony provision of 18 U.S.C. § 3553(a), which commands the court that it "shall impose a sentence sufficient, but not greater than

> necessary, to comply with the purposes" of punishment set out in the statute. In this case, for example, the special rule increased Lyles's punishment by eight levels, from 70–87 months to 140–175 months. A rule requiring courts to automatically double a sentence based on a fictional loss multiplier is a rule that may well produce a sentence greater than necessary to achieve punishment's aims. The parties have not raised, briefed, or argued this point, and we find no cases on the issue. Hence we only note the problem but do not decide it.

United States v. Lyles, 506 Fed.Appx. 440, 444 (6th Cir. 2012) (footnote omitted).

Even the guidelines themselves recognize that cases involving an unusually high number of victims risk exposure to a loss amount that overstates the seriousness of the offense:

> (C) Downward Departure Consideration — There may be cases in which the offense level determined under this guideline substantially overstates the seriousness of the offense. In such cases, a downward departure may be warranted.
>
> For example, a securities fraud involving a fraudulent statement made publicly to the market may produce an aggregate loss amount that is substantial but diffuse, with relatively small loss amounts suffered by a relatively large number of victims. In such a case, the loss table in subsection (b)(1) and the victims table in subsection (b)(2) may combine to produce an offense level that substantially overstates the seriousness of the offense. If so, a downward departure may be warranted.

USSG 2B1.1, application note 19, C.

In the spirit of § 3553's parsimony clause, we identify three factors the Court should consider under § 3553(a) that indicate that a sentence of 45 months is "sufficient, but not greater than necessary": (i) the disparate punishment a sentence greater that 45 months would affect on Mr. Baratov when compared to "defendants with similar records who have been found guilty of similar conduct," (§ 3553 (a)(6)); (ii) the minimal to non-existent nexus Mr. Baratov's conduct had to the United States; and (iii) Mr. Baratov's extremely young age at the time of the subject criminal conduct.

A. Additional Cases That Support Defendant's Requested Sentence of 45 Months

1. United States v. Phillips, 477 F.3d 215 (5th Cir. 2007)

In *United States v. Phillips*, the 22-year-old defendant hacked into a secure server at the University of Texas and instituted a computer program that allowed him to acquire personal information and data of more than 45,000 prospective students, donors and alumni over a 14-month period. *Id.* at 218. "He succeeded in infiltrating hundreds of computers, including machines belonging to other UT students, private businesses, U.S. Government agencies, and the British Armed Services webserver. In a matter of months, Phillips amassed a veritable informational goldmine by stealing and cataloguing a wide variety of personal and proprietary data, such as credit card numbers, bank account information, student financial aid statements, birth records, passwords, and Social Security numbers." *Id*. at 217. At trial he was convicted of violating §1030 and §1028 (identity theft) and received a sentence of five years' probation, five hundred hours of community service, and restitution of $170,056. *Id*. at 218-19.

Like Phillips, Mr. Baratov was arrested when he was 22 years old. Unlike Phillips, Mr. Baratov has chosen to accept responsibility and not pursue a trial. Unlike in this case, the government never charged Mr. Phillips with aggravated identity theft.

Offense: Phillips was convicted of one count of 18 USC § 1030 and one count of 18 USC § 1028

Sentence: Probation

2. United States v. Cameron Lacroix 14-cr-10162 (D. Ct. of Mass., 2014)

The defendant was 25 years old at the time of the offense. According to a USDOJ press release, the defendant "hacked into computer networks around the country – including networks belonging to law enforcement agencies, a local police department and a local college – and obtaining

highly sensitive law enforcement data and altering academic records.[1] He also obtained stolen credit, debit and payment card numbers." At 25, the defendant was already a long time hacker well known to law enforcement. He gained notoriety at 18 years old for hacking celebrity Paris Hilton's cell phone, for which he served 11 months in juvenile detention.[2]

Through his hacking, the defendant obtained highly sensitive law enforcement data, including obtaining access into the email account of the Chief of a local police department. He also hacked into state law enforcement databases containing police reports, intelligence reports, arrest warrants, and sex offender information, altered his own and other students' academic records, and obtained over 14,000 stolen credit, debit, and payment card numbers. Gov. Sent. Mem. at 3 (Dkt. 25).

With respect to his guideline calculation, 18 points were assessed for loss amount, based on the provision of 2B1.1 (F)(i), which assessed $500 in loss for each of the 14,000 stolen credit, debit, and other payment card information victims. In agreeing to a below-guideline sentence, the Government specifically expressed its concern over the $500 per access device calculation, stating:

> His guidelines are driven in large part by the 14,000 stolen access devices and the $500 per access device formula set forth in the USSG commentary. The government believes that the $7 million loss amount dramatically overstates the actual damage that Lacroix caused. First, it is not clear how many of the 14,000 cards were usable. And Courts have held that, for sentencing purposes, the $500 loss per card figure applies only to cards that are usable. See, e.g., United States v. Onyesoh, 764 F.3d 1157, 1160 (9th Cir. 2012). Furthermore, there is no evidence that Lacroix attempted to re-sell the stolen payment card data on the black market or elsewhere.
>
> Nevertheless, in the plea agreement, the government has agreed to recommend a 48-month sentence, which is almost half of Lacroix's guidelines range of 100-125 months. The government is seeking a variance because it believes that the guidelines calculation overstates the seriousness of the offense and does not take into account Lacroix's personal characteristics.

---

[1] https://www.justice.gov/opa/pr/massachusetts-man-pleads-guilty-computer-hacking-and-credit-card-theft (last visited May 18, 2018)

[2] https://www.bizjournals.com/boston/news/2014/06/02/hacker-whose-exploits-included-invading-paris.html (last visited May 18, 2018).

> Furthermore, although Lacroix hacked into many networks, the government has not identified damage that he caused, other than by changing grades at Bristol Community College. Moreover, the government is not aware of other instances in which Lacroix sold, or otherwise profited from, his access to the networks he hacked. Rather, he essentially "hoarded" the fruits of his hacking activities.

Id. at 6.

The same mitigating factors that the Government highlighted in *Lecroix* are prevailing in the instant matter. There is no evidence that significant harm was caused by any of Mr. Baratov's 11,000 hacks. Further, Mr. Baratov never harvested, sold, or other wise profited from his hacks other than the trivial $100 payment he received for hacking an account. Despite having the means to search the hacked accounts for profitable information and, at the very least, re-sell the credentials to cybercriminals on the web, Mr. Baratov never did so.

Offenses: 18 U.S.C. §§ 1030(a)(2), 1030(a)(5), 1029(a)(3).

Guidelines: 100-125 (Criminal History Category of IV).

Sentence: Agreed upon sentence of 48 months.

3. United States v. Knight 14-cr-00074 (N. D. Oklahoma, 2014)

The defendant, a 27-year-old member of the United States Navy, was the leader of a team of hackers. According to a USDOJ press release, the team of hackers: "conspired to hack computers and computer systems as part of a plan to steal identities, obstruct justice, and damage a protected computer."[3] The team hacked AT&T and downloaded over 7,500. Gov. Sent. Mem. at 3 (Dkt. 44) individuals' mobile phone numbers, users' records containing email addresses, full names, and mobile phone numbers with carrier names, addresses, and email addresses. The team also hacked the Toronto Police Service and downloaded more than 2,500 (*id*. at 4) usernames and passwords to police officer systems, including administrators. The defendant also obtained email addresses and names of

[3] https://www.justice.gov/usao-ndok/pr/former-navy-nuclear-system-administrator-charged-hacking-united-states-navy-and (last visited May 18, 2018)

citizens who have offered police tips through the department's hotline. The data stolen also included 500 police informants' names, addresses, phone numbers, email addresses, suspect descriptions, and police reports. *Id*.

The team also hacked into the NAVY-SWM's database and disclosed stolen personal data from the hack. The website was shut down as a result, and 700 deployed overseas service members could not access logistical support for transfers for more than 10 weeks. *Id*. at 5. The NAVY sustained more than $500,000 in loss to assess the damage from the hack and pay contractors and employees for their time devoted to the repair. The defendant also coordinated 20 other notable hacks, including the U.S. Department of Homeland Security, Montgomery Police Department, and the World Health Organization.

Offense: Knight pled guilty to one count of 18 USC § 371.

Guidelines: 46-57 months.

Sentence: 24 months.

4. United States v. Goodin 06-cr-00186 (C.D. Cal., 2007)

The defendant was 47 years old at the time of the offense, with one prior misdemeanor for battery. The defendant sent emails to AOL users purporting to be from the AOL Billing Department, requesting credentials and other personal information. The defendant used this information to steal money from his victims. *See* Gov. Sent. Mem. at 1 (Dkt. 115) The defendant's loss amount ultimately grew to more than $1 million, based mostly on damage caused to the service provider in investigating and repairing damage from his hacks. *Id*. at 8.

The court also applied sentence enhancements for mass marketing and failure to appear, bringing his adjusted offense level to 27, after a jury trial. Prior to trial, the defendant declined an offered sentence of 36 months incarceration.

Offenses: 15 U.S.C. §§ 7701-13; 18 U.S.C. §§ 1343 (3 counts) 1037, 1029(a)(2), 1029(a)(3), 1028A(a)(1), 2320(a), 1512(d)(1), 3146(a), 3146(b)(1)(A)(iii). *Good v. United States*, 2010 U.S. Dist. LEXIS 79911 *1-2 (CDC, 2010)

Guidelines: 70-87 months; plus consecutive 24 under 1028A.

Sentence: Offer of 36 months pre-trial; sentenced after trial to 94 months.

5. United States v. Jeanson James Ancheta, 2:05-cr-01060 (C.D. Cal. May 26, 2006)

In *United States v. Jeanson James Ancheta*, the 22-year-old defendant hijacked approximately half a million computer systems by taking advantage of flaws in Microsoft's Windows operating system, sold DDOS bots online (10,000 at a time) that would allow for DDOS attacks, caused an actual monetary loss of $14,611.54 (which was ordered as restitution) and following his plea to §1030, received a sentence of 57 months. *See* Minutes of Sentencing (Dkt. 34); Judgment and Commitment (Dkt. 35). Like Mr. Baratov, Ancheta was young when he committed the crimes and the amount of restitution for Ancheta is relatively low compared to many of the other hacking cases. However, unlike Mr. Baratov, who allegedly hacked approximately 11,000 emails, Ancheta's malicious code affected nearly half a million computer systems.

Offense: Ancheta pled guilty to two counts of 18 USC § 371 and two counts of 18 USC § 1030

Sentence: 57 months

B. The Government's Statistical Analysis Provides No Information And Cannot Be Considered

The Government identifies 14 non-government-sponsored sentences and performs various mathematical comparisons to support its argument that a sentence of 94 months is not disproportionate to defendants that have similar records and were found guilty of similar conduct to Mr. Baratov. *See* Dkt. 43 at 13-15. Unfortunately, the Government's identification of these 14 non-government-sponsored sentences does not include the names of the cases or any details related to the offenses committed. The reader has no clue what the justifications for the identified sentences are and how

such factors compare to the circumstances of Mr. Baratov's case. Thus, the Government's analysis is useless.

The Government argues: "The average of all 14 sentences is 318 months of imprisonment. The average without the two endpoints is 62.5 months of imprisonment. As detailed previously in the United States Sentencing Memorandum […] Defendant Baratov's egregious, extensive, and reprehensible conduct makes it necessary that his sentence fall on the serious side of the spectrum." Dkt. 43 at 14. However, without some comparison of Mr. Baratov's conduct to the conduct in the 14 cases the Government identifies, there is no basis to conclude that Mr. Baratov's conduct was "egregious, extensive, and reprehensible." Put another way, the Government cannot compare Mr. Baratov to defendants "who have been found guilty of similar conduct" without describing the conduct in the cases it identifies.

Void of any detail, the statistics alone do little to inform the Court with respect to an appropriate sentence for Mr. Baratov. For example, one of the median sentences – when the 14 cases are ranked from longest to shortest by sentence (*see* table on Dkt. 43 at 13-14) – includes a case that has an offense level of 13 with 0 loss amount, but resulted in a sentence of 60 months. Clearly the facts of such a case are necessary to explain the extremely high sentence, which is more than 3 times the guideline range. Similarly, the case most similar to Mr. Baratov's (on paper) is the other median case, which has a loss amount of +18, a final offense level of 26, a Criminal History Category of 1, and a sentence of 51 months. Although such a sentence is 43 months shorter than what the Government is requesting for Mr. Baratov, the absence of any facts relevant to the case renders Mr. Baratov unable to compare his case in a useful manner.

C. The Government's Cases Support the Defendant's Requested Sentence of 45 Months

The Government identifies 14 specific hacking cases it claims justify a 94 month sentence for Mr. Baratov. These cases are each distinguishable from Mr. Baratov's in important respects.

However, it cannot be overstated that virtually all the defendants in the Government's cited cases were older than Mr. Baratov during their commission of their crimes.

i. The Government's Carding Cases

United States v. Gonzalez, *Seleznev, and Salcedo* need not be addressed, as the Government's description of the extreme factual differences render them useless to inform the Court of the appropriate sentence for Mr. Baratov. The other cases are addressed as follows:

United States v. Butler, 07-cr-332-MBC (W.D. Pa. Feb. 12, 2010) is distinguishable because the 35-year-old defendant was found in possession of more than 1.8 million stolen credit card numbers (1,166,851 Visa cards; 453,154 Mastercard; 164,877 American Express; and 49,362 Discover cards), hacked into thousands of computers, stipulated to a loss of $86.4 million (representing the total of the fraudulent charges on the credit card accounts possessed by the defendant), caused an actual loss of $27,500,000 (which was ordered as restitution), created a website for the purpose of recruiting other cyber-criminals, and was ultimately sentenced to 156 months, only 5 years more than the Government's recommended sentence for Mr. Baratov. *See* Judgment As To Max Ray Butler (Dkt. 70); Gov. Sent. Mem. at 1 (Dkt. 66)

United States v. Bendelladj, 1:11-cr-00557-AT-AJB (N.D. Ga. Apr. 20, 2016) is distinguishable because the 23-year-old defendant intentionally stole financial info such as banking credentials, credit card info and PINS, from 500,000 people and caused millions in loss to individuals and institutions. Dkt. 43 at 6. Here, Baratov obtained the email passwords only (no financial information), of approximately 11,000 people, which is 1/45th the number of people affected by the defendants in *Bendelladj*. Moreover, unlike the millions in losses to individuals and institutions, the Government in this case has been unable to prove that Baratov caused any actual loss. Despite the actual and extensive harm in *Bendelladj*, the district court imposed a below guideline sentence of 180 months. *Id*.

United States v. Tverdokhlebov, 1:17-cr-9-TSE (E.D. Va. July 10, 2017) is distinguishable because the 27-year-old defendant in that case possessed 40,000 stolen credit cards and controlled 500,000 infected computers. Dkt. 43 at 7. He sold the stolen financial info to cybercriminals so that those cybercriminals could then place fraudulent charges on the 40,000 stolen credit cards. *Id.* Here, Mr. Baratov did not indiscriminately sell the passwords he phished to any requesting cybercriminal, nor did he effect anywhere near 500,000 computers and 40,000 credit cards. Tverdokhlebov was sentenced to 110 months, only 16 months more than the Government's requested sentence for Mr. Baratov.

ii. The Government's Non-Carding Cases

United States v. Makwana, 1:09-cr-00043-JFM (D. Md. Dec. 17, 2010) is distinguishable because the 35-year-old defendant was convicted after trial for intending and attempting to install a malicious code at Fannie Mae that would have destroyed all data, including financial, securities, and mortgage info, on 5,000 computer servers, substantially jeopardizing the safety and soundness of a financial institution. The defendant also caused actual monetary harm in excess of $70,000, and the government projected a loss of 47.7 million dollars in revenue had the malicious code been executed. Dkt. 43 at 7; *See also* Resp. in Opp. by USA as to Makwana Motion to Vacate Under 28 U.S.C. 2255 at 2 (Dkt. 107); *United States v. Makwana*, 445 F App'x 671, 674, n * (4th Cir 2011). Makwana was sentenced to 41 months in prison, the bottom of the guidelines. Dkt. 43 at 8.

United States v. Chaney, 2:11-cr-00958-SJO (C.D. Cal. Dec. 17, 2012) is distinguishable because the 34-year-old defendant, who had a prior felony, hacked into 60 email accounts and stole nude photos and forwarded them to third parties resulting in public disclosure. The defendant also caused actual monetary harm in the amount of $160,821.40, caused significant physical harm to at least one victim, continued his hacking activities after the FBI executed a search warrant and seized his computer, was facing child pornography charges in another district, and was deemed to be at a high

risk of recidivism. *See* Gov. Sent. Mem. at 7 (Dkt. 36); Case Summary (Dkt. 4). "Prior to hacking celebrity email accounts, defendant had hacked into the e-mail accounts of other female victims, including one who was underage for part of the 11 years that defendant was victimizing her." *See* Gov. Sent. Mem. at 8 (Dkt. 36) He also had child pornography videos on his computer.

Notably, the government stated that "as part of his plea agreement in this case, defendant received the benefit of the government forgoing the aggravated identity theft counts charged in this case and the mandatory, consecutive, 24-month sentence that went with them." *Id*. at 7. Chaney was sentenced to 120 months in prison. Dkt. 43 at 8.

United States v. Musacchio, 3:10-cr-00308-P-1 (N.D. Tx. Sept. 5, 2013) is distinguishable because the 59-year-old defendant committed corporate espionage following his departure as the CEO and president of a third-party logistics company that caused approximately 1 million in loss. Dkt. 43 at 9; *United States v. Musacchio*, 590 F App'x 359, 362 (5th Cir 2014). Musacchio was sentenced to 63 months, which was the bottom of the guideline range. *Id*.

United States v. Laoutaris, 3:13-cr-00386-B-1 (N.D. Tx. Apr. 15, 2016) is distinguishable because the 37-year-old defendant deleted and/or damaged hundreds of computer, user, and e-mail accounts of employees of a large, international law firm (which also therefore cause harm to the law firm's clients), caused actual loss of $1,697,800 (which was ordered as restitution), attempted to obstruct justice by lying under oath at trial, and was found guilty after trial. *Id*. at 9; *See* Judgment (Dkt. 103) Despite the actual loss of nearly $1.7 million, and obstruction of justice, the defendant in Laoutaris was sentenced to 115 months, only 21 months more than the 94 months the Government requests in this case for Mr. Baratov. *Id*.

United States v. Correa, 4:15-cr-00679 (S.D. Tx. July 18, 2016) is distinguishable because the 30-year-old defendant in that case (who was sentenced to 46 months), intended a loss of $1.7 million, caused an *actual monetary loss* of *$279,038.65* (which was ordered for restitution), and, despite the

fact that he used victims' passwords to gain unauthorized access to their email and personal online data accounts, he was not charged with aggravated identity theft and the government recommended a 46-month sentence, the bottom of the guidelines. *See* Minute Entry for Sentencing on 7/18/2016.

Here, although the number of accounts Mr. Baratov phished were far greater, he never intended to cause monetary loss and the Government cannot prove that any actual monetary loss occurred. Additionally, in Correa, the government's discretion in choosing not to charge the defendant with aggravated identity theft despite the appropriateness of the charge, made a substantial difference in Correa's ultimate sentence.

United States v. Livingston, 2:15-cr-00626-WJM (D.N.J. Feb. 14, 2017) is distinguishable because the 26-year-old defendant in that case, who was sentenced to 24 months, to run consecutive with 24 months on an aggravated identity theft charge (total term of 48 months, 9 months below the guidelines range), participated in a conspiracy to use *hundreds of thousands of real people's hacked email accounts without their permission* to send out advertising messages for a profit, and caused a total actual loss of *$64,529.74* (ordered for restitution), and earned an agreed upon amount of $1,346,442 (order of forfeiture). *See* First Mot. in Lim. to Admit 404(b) by USA, at 1 (Dkt. 39); Final Order of Restitution (Dkt. 75); Second Corrected Amended Judgment (Dkt. 76). Notably, defendant Livingston's co-conspirator, Tomasz Chmielarz, who authored hacking tools and other computer code used to facilitate the crime and also provided Livingston with hacked email accounts, was sentenced to two years of probation. *See* Minute Entry for Sentencing (Dkt. 63)

United States v. Lostutter, 5:16-cr-00062 (E.D. Ky. Mar. 8, 2017) is distinguishable because the 27-year-old defendant in that case defamed a blog website operator as a child pornographer and director of a "rape crew," threatened to do the same to a list of high school students, invaded the privacy of adult women by publicly posting their emails containing nude photographs, identified himself as a member of a computer hacking organization called Anonymous, violated his conditions of

release within days by using the internet to threaten others, and repeatedly obstructed justice by lying to the FBI committing perjury in sworn testimony before the Court. *See* Gov. Sent. Mem. at 2-3 (Dkt. 101). Despite Lostutter's intentionally malicious conduct designed to threaten and harm innocent individuals, the government offered him a plea in which the two §1030 counts would be dismissed and Lostutter would be required to plead guilty to a §371 conspiracy count and a §1001 count for false statements. Lostutter was ultimately sentenced to 24 months in prison. *See* Judgment Upon Plea of Guilty (Dkt. 109) The government never charged the defendant with aggravated identity theft.

United States v. Fernandez, 14-cr-0277-GPC (S.D. Cal. Jan. 19, 2018) is distinguishable because the 35-year-old defendant specifically victimized approximately 250 individuals by draining their retirement and brokerage accounts. Dkt. 43 at 11. The victims suffered significant financial harm that affected their livelihoods, resulting in a total actual loss between $400,000 and $1 million. *Id*. The district court imposed a sentence of 129 months, below the applicable guideline range. *Id*.

D. Other Factors Under §3553(a) Mandate a Below Guidelines Sentence for Mr. Baratov

The Government admits that 9,000 of Mr. Baratov's hacking activity was performed from Canada, and resulted in hacks of Russian-based webmail accounts located in Russia. Thus, more than 80% of the relevant conduct responsible for driving up Mr. Baratov's sentence has no nexus to the United States. The Government would not have jurisdiction to prosecute Mr. Baratov substantively for any of these 9,000 hacks (*United States v. Perlaza*, 439 F.3d 1149 (9th Cir 2006)); however, pursuant to USSG §1B1.13, the Court is permitted to consider such conduct as "relevant conduct."

The Court should consider the lack of nexus to the United States a major mitigating factor in determining Mr. Baratov's sentence. For example, if we exclude the 9,000 hacks having no nexus to the United States, we are left with 2,000 hacks performed on United States based web mail services. Applying the $500 multiplier, the resulting loss amount is $1 million, and per the USSG. The addition

of 14 points is required resulting in an offense level of 23, rendering the appropriate guideline range 46-57 months.

Mr. Baratov's youth is an additional factor to consider under § 3553(a). Mr. Baratov is younger than any defendant identified in the cases the Government and defense have identified. Further, the Government admits that conduct from three years before Mr. Baratov's 18th birthday was factored into his loss amount calculation. Dkt. 36 at 1.

CONCLUSION

In light of the foregoing, Defendant respectfully requests the Court impose a sentence of 45 months, 3 years supervised release, and no restitution.

Dated: New York, New York
May 18, 2018

s/Andrew Mancilla
Andrew Mancilla, Esq.

s/Robert Fantone
Robert Fantone, Esq.

cc: Jeffrey Shih (via ECF)